

preparing synthesized data wherein the substantive data unit and the sample data unit are synthesized, and distributing the synthesized data.

2. (ONCE AMENDED) The data management method set forth in claim 1, further comprising:

enabling access to the synthesized data by separating the authorization information from the sample data unit ; and

restoring from the authorization information a decryption key for decrypting the substantive data unit.

3. (ONCE AMENDED) The data management method set forth in claim 1, wherein the sample data is image data contained in the digital content and at least one process among image processing, resizing, compressing and a γ -compensation is executed on the image data.

4. The data management method set forth in claim 1, wherein the sample data is index data for representing the substantive data unit.

5. (ONCE AMENDED) The data management method set forth in claim 4, wherein the synthesized data contains a plurality of substantive data units based on a plurality of digital content items, and contains a plurality of sample data units corresponding to the plurality of substantive data units; and wherein each sample data is linked with respective corresponding ones of the plurality of substantive data units.

6. (ONCE AMENDED) The data management method set forth in claim 1, wherein the sample data units is data structuralized in one of JPEG and MPEG formats, and the synthesized data is prepared by add-on synthesizing the substantive data unit to the sample data unit using the format of the sample data unit.

7. (ONCE AMENDED) The data management method set forth in claim 1, wherein the encryption key is at least one of user identification information, equipment identification information loaded in user-employed computers, CPU identification information loaded in the user-employed computers, and identification information unique to digital-content-storing recording media.

8. (ONCE AMENDED) The data management method set forth in claim 1, wherein the encryption key is identification information common to a plurality of users.

9. (ONCE AMENDED) The data management method set forth in claim 1, wherein the encryption key is at least one of identification information unique to distributors of the digital content, and identification information unique to authors of the digital content.

10. (ONCE AMENDED) The data management method set forth in claim 7, wherein a decryption key for decrypting the encrypted encryption key is common to an encryption key for encrypting the digital content, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.

11. (ONCE AMENDED) The data management method set forth in claim 8, wherein a decryption key for decrypting the encrypted encryption key is common to an encryption key for encrypting the digital content, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.

12. (ONCE AMENDED) The data management method set forth in claim 9, wherein a decryption key for decrypting the encrypted encryption key is common to an encryption key for encrypting the digital content, the decryption key being a shared key based on exclusive on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.

13. (ONCE AMENDED) The data management method set forth in claim 7, wherein digital content distributors encrypt the encryption key employing a secret key, and the users decrypt the encrypted encryption key employing a public key provided in advance from the digital content distributors, using public key cryptography.